

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-339608

(P 2 0 0 2 - 3 3 9 6 0 8 A)

(43) 公開日 平成14年11月27日 (2002. 11. 27)

(51) Int. Cl. ⁷	識別記号	F I	テ-マコード (参考)
E05B 49/00		E05B 49/00	J 2E250
G06F 15/00	330	G06F 15/00	G 5B085

審査請求 有 請求項の数10 O L (全9頁)

(21) 出願番号 特願2001-147555 (P 2001-147555)

(22) 出願日 平成13年5月17日 (2001. 5. 17)

(71) 出願人 500376807

有限会社アクセント

東京都荒川区東日暮里1丁目5番15-201
号 アガワマンション

(72) 発明者 洲鎌 誠

東京都荒川区東日暮里1丁目5番15-201
号 アガワマンション 有限会社アクセ
ント内

(74) 代理人 100087859

弁理士 渡辺 秀治 (外1名)

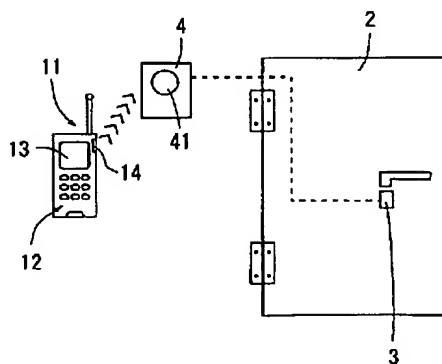
最終頁に続く

(54) 【発明の名称】 携帯端末及び認証システムならびに認証方法

(57) 【要約】

【課題】 低コストでかつある程度のセキュリティ性がある認証方法で個人を識別し、容易に開錠やコンピュータのログイン等をできる携帯端末及び認証システムならびに認証方法を提供する。

【解決手段】 少なくとも1つ以上の識別記号を保存する記憶手段（図示省略）と、識別記号を送信する送信手段14とを備え、電子錠3を備えたドア2に接続された受信装置4に、記憶手段に保存された識別記号の少なくとも1つであって、受信装置4に保存されている識別記号と比較させ一致したときは開錠し、不一致のときは開錠しないこととなる識別記号を送信可能にしている。



【特許請求の範囲】

【請求項 1】 少なくとも 1 つ以上の識別記号を保存する記憶手段と、上記識別記号を送信する送信手段とを備え、電子錠を備えたドアに接続された受信装置に、上記記憶手段に保存された識別記号の少なくとも 1 つであって、上記受信装置に保存されている識別記号と比較させ一致したときは開錠し、不一致のときは開錠しないこととなる識別記号を送信可能にしたことを特徴とする携帯端末。

【請求項 2】 少なくとも 1 つ以上の識別記号を保存する記憶手段と、上記識別記号を送信する送信手段とを備え、コンピュータに接続された受信装置に、上記記憶手段に保存された識別記号の少なくとも 1 つであって、上記受信装置に保存されている識別記号と比較させ一致したときは上記コンピュータへのログインをし、不一致のときは上記コンピュータへのログインをしないこととなる識別記号を送信可能にしたことを特徴とする携帯端末。

【請求項 3】 少なくとも 1 つ以上の識別記号を保存する記憶手段と、上記識別記号を送信する送信手段とを備え、出退勤認識装置に接続された受信装置に、上記記憶手段に保存された識別記号の少なくとも 1 つであって、上記受信装置に保存されている識別記号と比較させ一致したときは出退勤を記録し、不一致のときは出退勤の記録をしないこととなる識別記号を送信可能にしたことを特徴とする携帯端末。

【請求項 4】 少なくとも 1 つ以上の識別記号を保存する記憶手段と、上記識別記号を送信する送信手段とを備え、住民票登録管理装置に接続された受信装置に、上記記憶手段に保存された識別記号の少なくとも 1 つであって、上記受信装置に保存されている識別記号と比較させ一致したときは上記住民票登録管理装置から当該携帯端末の所有者に関する情報を引き出し、不一致のときは上記情報を引き出せないこととなる識別記号を送信可能にしたことを特徴とする携帯端末。

【請求項 5】 少なくとも 1 つ以上の識別記号を保存する記憶手段と、上記識別記号を送信する送信手段とを備えた携帯端末であって、電子錠を備えたドアの開錠または閉錠の少なくとも一方を行うための識別記号、コンピュータへのログインのための識別記号、当該携帯端末の所有者の出退勤を記録させるための識別記号、および住民票登録管理装置から当該携帯端末の所有者に関する情報を引き出すことが可能な識別記号を上記記憶手段に保存し、かつ受信装置側に送信可能としたことを特徴とする携帯端末。

【請求項 6】 前記識別記号の送信は、赤外線通信または無線通信にて行われることを特徴とする請求項 1 から 5 のいずれか 1 項記載の携帯端末。

【請求項 7】 前記識別記号を送信するための送信部を差し込み可能とした端子装置を備え、この端子装置に当

該携帯端末の上記送信部を差し込むことにより前記識別記号の送信を行うようにしたことを特徴とする請求項 1 から 5 のいずれか 1 項記載の携帯端末。

【請求項 8】 パスワードを入力して前記受信装置に当該携帯端末の所有者を識別させた後に、この受信装置に接続された装置に所定の動作を開始させることを特徴とする請求項 1 から 7 のいずれか 1 項記載の携帯端末。

【請求項 9】 少なくとも 1 つ以上の識別記号を保存する記憶手段と、上記識別記号を送信する送信手段とを備えた携帯端末と、この携帯端末から送信される上記識別記号を受信する受信装置とを備え、上記携帯端末から上記受信装置へ送信された識別記号を上記受信装置が認証した後に、電子錠の開錠を行うこと、コンピュータへのログインをさせること、出退勤認識装置に上記携帯端末の所有者の出退勤を認識させること及び住民票登録管理装置から上記携帯端末の所有者に関する情報を引き出すことの少なくともいずれか 1 つを可能としたことを特徴とする認証システム。

【請求項 10】 少なくとも 1 つ以上の識別記号を保存する記憶手段と、上記識別記号を送信する送信手段とを備えた携帯端末から、受信装置に対して上記識別記号を送信することによってこの受信装置に上記識別記号の認証を行わせ、この認証に基づいて、電子錠の開錠を行うこと、コンピュータのログインをさせること、出退勤認識装置に上記携帯端末の所有者の出退勤を認識させること及び住民票登録管理装置から上記携帯端末の所有者に関する情報を引き出すことの少なくともいずれか 1 つを行うことを特徴とする認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、個人の認証機能を有する携帯端末、及び携帯端末を用いた認証システム、ならびに携帯端末を用いた認証方法に関するものである。

【0002】

【従来の技術】従来より、車や家の鍵を見知らぬ人に開けられ、その内部に進入された上に盗難等の被害に遭うというケースは多々ある。このような被害を防止するために、セキュリティの高い鍵が種々開発されている。例えば、指紋認証や声紋認証等のバイオメトリクスを利用した鍵や、パスワード入力を経た鍵等である。

【0003】なお、これらの鍵は、鍵を開ける人を認証した上で開錠するという点で共通する。すなわち、特定の人しか鍵を開けることができないような工夫がなされている。指紋認証や声紋認証等のバイオメトリクスを利用する鍵は、その人の身体的な特徴（指紋や声紋）を予め登録しておき、その登録された身体的な特徴を有する人のみが開錠できる仕組みとなっている。すなわち、登録された身体的特徴を持つ人以外は、その進入が拒まれる（開錠ができない）仕組みとなっており、非常にセキ

セキュリティ性が高い。

【0004】また、パスワード入力を課す鍵は、特定の人しか知らないパスワードを開錠の際に入力する必要があり、パスワードを知らない人は内部へ進入できないような仕組みとなっている。したがって、パスワードを他人に知られないように管理しておけば、これも非常にセキュリティ性は高い。

【0005】このような各種認証は、鍵の開錠以外の分野でも種々応用されている。例えば、コンピュータを用いてネットワークにログインしたり、あるいは単にアプリケーションを起動させたりする際に、パスワード入力を課すような仕組みとなっているものがある。また、例えば、銀行のＡＴＭでも、銀行が特定の個人に対して発行したカードを差し込み、さらに暗証番号を入力しないとＡＴＭが機能しないようになっている。

【0006】

【発明が解決しようとする課題】上述したように、開錠やコンピュータのログイン時等において、個人の認証を行う方法が種々実用化されている。しかし、それぞれに課題を有している。すなわち、指紋認証や声紋認証等のバイオメトリクスを利用するものに関しては、その設備が非常に高度で高コストとなる。したがって、一般的な家庭の家やマンションや車の開錠時の認証方法としては、まだまだ現実的ではない。

【0007】さらに、開錠時等にパスワード入力を課すものに関しては、その入力コードや暗証番号等を暗記しておく必要がある。正当な権利者であっても、そのパスワードを忘れてしまった場合には、開錠やログインができない。しかも、その鍵やログイン等、各認証毎にパスワードが異なるため、パスワードを忘れてしまうことも多い。しかも、パスワードは、他人に知られないように管理する必要がある。このように、パスワードの管理（暗記及び盗難防止）は、容易ではなく、非常に面倒であるという問題がある。

【0008】本発明は、上述の問題を解消するためになされたものであり、低コストでかつある程度のセキュリティ性がある認証方法で個人を識別し、容易に開錠やコンピュータのログイン等をできる携帯端末及び認証システムならびに認証方法を提供することを目的とする。

【0009】

【課題を解決するための手段】上記した目的に鑑みて、本発明の携帯端末は、少なくとも１つ以上の識別記号を保存する記憶手段と、識別記号を送信する送信手段とを備え、電子錠を備えたドアに接続された受信装置に、記憶手段に保存された識別記号の少なくとも１つであって、受信装置に保存されている識別記号と比較させ一致したときは開錠し、不一致のときは開錠しないこととなる識別記号を送信可能にしたことを特徴としている。

【0010】そのため、携帯端末に電子錠を開錠するための識別記号を登録しておけば、携帯端末を鍵の代わり

として利用することができる。しかも、指紋認証等が可能な高コストの設備を取り付けたり、パスワード入力等、人の暗記に頼らずに、確実に開錠時の個人の認証を行うことができる。したがって、ある程度のセキュリティ性と利便性とを兼ね備えることができる。

【0011】また、他の本発明の携帯端末は、少なくとも１つ以上の識別記号を保存する記憶手段と、識別記号を送信する送信手段とを備え、コンピュータに接続された受信装置に、記憶手段に保存された識別記号の少なくとも１つであって、受信装置に保存されている識別記号と比較させ一致したときはコンピュータへのログインをし、不一致のときはコンピュータへのログインをしないこととなる識別記号を送信可能にしたことを特徴としている。

【0012】そのため、携帯端末にログイン用の識別記号を登録しておけば、携帯端末をログイン時の個人認証装置として利用することができる。しかも、指紋認証等が可能な高コストの設備を取り付けたり、パスワード入力等、人の暗記に頼らずに、確実な個人認証を行うことができる。したがって、ある程度のセキュリティ性と利便性とを兼ね備えることができる。

【0013】また、他の本発明の携帯端末は、少なくとも１つ以上の識別記号を保存する記憶手段と、識別記号を送信する送信手段とを備え、出退勤認識装置に接続された受信装置に、記憶手段に保存された識別記号の少なくとも１つであって、受信装置に保存されている識別記号と比較させ一致したときは出退勤を記録し、不一致のときは出退勤の記録をしないこととなる識別記号を送信可能にしたことを特徴としている。

【0014】そのため、携帯端末に識別記号を登録しておけば、携帯端末を社員証として利用することができる。すなわち、携帯端末による識別記号の送信動作を、従来のタイムカードへの出退勤時刻の入力や通用門での社員証提示の代わりに動作とすることができる。しかも、指紋認証等が可能な高コストの設備を取り付けたり、パスワード入力等、人の暗記に頼らずに、確実な個人認証を行うことができる。したがって、ある程度のセキュリティ性と利便性とを兼ね備えることができる。

【0015】また、他の本発明の携帯端末は、少なくとも１つ以上の識別記号を保存する記憶手段と、識別記号を送信する送信手段とを備え、住民票登録管理装置に接続された受信装置に、記憶手段に保存された識別記号の少なくとも１つであって、受信装置に保存されている識別記号と比較させ一致したときは住民票登録管理装置から当該携帯端末の所有者に関する情報を引き出し、不一致のときは情報を引き出せないこととなる識別記号を送信可能にしたことを特徴としている。

【0016】住民票の発行等を自治体に申請する場合、住所や氏名等の各種情報を所定の用紙に記入してこれを受付窓口に提出する必要がある。しかし、本発明によれ

ば、携帯端末に識別記号を登録しておけば、その識別記号を携帯端末から送信するだけで、上述の申請を行えるようになる。しかも、指紋認証等が可能な高コストの設備を取り付けたり、パスワード入力等、人の暗記に頼らずに、確実な個人認証を行うことができる。したがって、ある程度のセキュリティ性と利便性とを兼ね備えることができる。

【0017】また、他の本発明の携帯端末は、少なくとも1つ以上の識別記号を保存する記憶手段と、識別記号を送信する送信手段とを備えた携帯端末であって、電子錠を備えたドアの開錠または閉錠の少なくとも一方を行うための識別記号、コンピュータへのログインのための識別記号、当該携帯端末の所有者の出退勤を記録させるための識別記号、および住民票登録管理装置から当該携帯端末の所有者に関する情報を引き出すことが可能な識別記号を記憶手段に保存し、かつ受信装置側に送信可能としたことを特徴としている。

【0018】従来より、電子錠の開錠、コンピュータのログイン、出退勤記録、住民票等の申請等は、その動作を行う個人を特定する必要がある、セキュリティ性が求められるが、一方で簡便さも要求される。本発明によれば、携帯端末に上述の各動作を行うための識別記号をそれぞれ登録しておけば、電子錠の開錠等の種々の動作を、各識別記号を携帯端末から送信するだけで行える。しかも、指紋認証等が可能な高コストの設備を取り付けたり、パスワード入力等、人の暗記に頼らずに、確実な個人認証を行うことができる。したがって、ある程度のセキュリティ性と利便性とを兼ね備えることができる。

【0019】また、他の発明は、上述の各携帯端末において、識別記号の送信は、赤外線通信または無線通信にて行われることを特徴としている。そのため、識別記号の送信を非接触で行うことができるので、離れた位置からでも電子錠の開錠等を行うことが可能となり、利便性がさらに高くなる。

【0020】また、他の発明は、上述の携帯端末において、識別記号を送信するための送信部を差し込み可能とした端子装置を備え、この端子装置に当該携帯端末の送信部を差し込むことにより識別記号の送信を行うようにしたことを特徴としている。そのため、識別記号の送信をより確実な動作で行うことができる。

【0021】また、他の発明は、上述の携帯端末において、パスワードを入力して受信装置に当該携帯端末の所有者を識別させた後に、この受信装置に接続された装置に所定の動作を開始させることを特徴としている。そのため、個人の認証に関して、簡便さはやや劣るが、セキュリティの質が向上する。

【0022】また、本発明の認証システムは、少なくとも1つ以上の識別記号を保存する記憶手段と、識別記号を送信する送信手段とを備えた携帯端末と、この携帯端末から送信される識別記号を受信する受信装置とを備

え、携帯端末から受信装置へ送信された識別記号を受信装置が認証した後に、電子錠の開錠を行うこと、コンピュータへのログインをさせること、出退勤認識装置に携帯端末の所有者の出退勤を認識させること及び住民票登録管理装置から携帯端末の所有者に関する情報を引き出すことの少なくともいずれか1つを可能としたことを特徴としている。

【0023】そのため、携帯端末に識別記号を登録しておけば、この携帯端末を利用して開錠やコンピュータのログイン等を行うことができる。しかも、指紋認証等が可能な高コストの設備を取り付けたり、パスワード入力等、人の暗記に頼らずに、確実に開錠時の個人の認証を行うことができる。したがって、ある程度のセキュリティ性と利便性とを兼ね備えることができる。

【0024】また、本発明の認証方法は、少なくとも1つ以上の識別記号を保存する記憶手段と、識別記号を送信する送信手段とを備えた携帯端末から、受信装置に対して識別記号を送信することによってこの受信装置に識別記号の認証を行わせ、この認証に基づいて、電子錠の開錠を行うこと、コンピュータのログインをさせること、出退勤認識装置に携帯端末の所有者の出退勤を認識させること及び住民票登録管理装置から携帯端末の所有者に関する情報を引き出すことの少なくともいずれか1つを行うことを特徴としている。

【0025】そのため、指紋認証等の構成が複雑な方法や、パスワード入力等による人の暗記に頼るという不安定な方法によらず、携帯端末に識別記号を登録しておくという簡単な方法で確実に開錠時等の個人の認証を行うことができ、この認証を利用して開錠やログインや住民票の発行等を行うことができる。したがって、ある程度のセキュリティ性と利便性とを両立できる。

【0026】

【発明の実施の形態】以下、本発明に係る各実施の形態の携帯端末及び認証システムならびに認証方法について、図面に基づいて以下に説明する。なお、以下の各実施の形態では、本発明において同じ機能を有するものは同一の符号を使用して説明するものとする。

【0027】以下に説明する第1の実施の形態の認証システムは、図1に示すように、携帯端末1を用いてドア2の電子錠3を開錠するものとなっている。すなわち、携帯端末1から送信される識別記号を電子錠3に接続された受信装置4が識別して、この携帯端末1の所有者を認証した後に、電子錠3を開錠する認証システムとなっている。なお、識別記号としては、番号のみで構成されるもの、番号と特殊記号で構成されるもの、特殊記号のみで構成されるものの3形態が存在する。

【0028】携帯端末1は、無線で音声データや文字データ等を送受信可能な携帯電話で構成されており、通常時は携帯電話としての機能を有するものである。すなわち、この携帯端末1は、データの送受信を行うための各

種回路及び記憶手段としてのメモリー（図示省略）を有している。そして、メモリーには、ドア 2 の電子錠 3 を開錠するための識別記号を保存することが可能となっている。また、携帯端末 1 は、無線通信電波を送受信する送受信部 11 と、入力キー 12 と、表示画面 13 と、赤外線でデータを送信可能な送信手段となる送信部 14 を有している。メモリーに保存された識別記号は、電子錠 3 を開錠する際に、利用者の操作により送信部 14 から赤外線を受信装置 4 に向けて送信される。

【0029】受信装置 4 は、赤外線データを受信可能な受信部 41 を備えていると共に、電子錠 3 に接続されている。この受信装置 4 は、所定の識別記号が所定の送信方法で送信されてくると、これを識別し認証するようになっている。すなわち、携帯端末 1 の所有者を電子錠 3 を開錠する正当な権利者として認識する。そして、認証したという結果を、電子錠 3 に送る。電子錠 3 は、携帯端末 1 から送信された赤外線信号を正当な識別記号であると受信装置 4 が認証したことにより開錠されるようになっている。この受信装置 4 は、電子錠 3 とは別体とせず、電子錠 3 の中に組み込んでも良い。また、電子錠 3 の例としては、家のドアの場合に限らず、車の錠、金庫の錠等、種々の錠に適用できる。

【0030】なお、ドア 2 の電子錠 3 を開錠するための識別記号を、携帯端末 1 のメモリーに登録し保存させる手順の一例について、図 2 を用いて説明する。

【0031】まず、利用者（携帯端末 1 の所持者）は、メニューキー及びカーソルキー等で構成される入力キー 12 を操作し、表示画面 13 に識別記号を登録するための画面を表示させる（ステップ S1）。そして、利用者は、ドア 2 の電子錠 3 を開錠するために必要な識別記号の入力を、登録画面上で入力キー 12 を用いて行う（ステップ S2）。これにより、識別記号が携帯端末 1 のメモリーに登録される（ステップ S3）。

【0032】なお、この例では、携帯端末 1 の利用者が、携帯端末 1 に識別記号を入力し記憶させる前に、受信装置 4 の販売業者（もしくは取り付け業者）から予めその識別記号を教えてもらい、これを手作業で入力するものとする。しかし、例えば、識別記号を業者から携帯端末 1 に E メールで送ってもらうようにしても良い。また、受信装置 4 の固有の ID 及びそれに対応する識別記号等を管理する管理装置を業者が備え、この管理装置に携帯端末を直接（無線または有線で）接続してメモリーに識別記号を入力してもらうようにしても良い。さらには、最初に仮 ID を発行してもらい、その仮 ID で受信装置 4 と通信し、その通信時に自己にとって都合の良い他の本 ID を入力するようにしても良い。

【0033】加えて、携帯端末 1 の出荷時には、例えば、上述の開錠用の識別記号を ID としては意味をなさない「0000」のような統一番号としておいても良い。そして、利用者が当該携帯端末 1 を鍵として自分で

実際に使用する前に、携帯端末 1 の開錠用の固有の識別記号を入力し、これに合わせて受信装置 4 側の識別記号も携帯端末 1 からの識別記号の送信で開錠できるように設定するようにしても良い。

【0034】またさらに、電子錠 3 を識別記号の送信および認証だけで開錠する構成とせず、従来型の金属製の鍵を鍵穴に差し込んでから識別記号の送信をすると、鍵が開くように構成しても良い。また、従来型の金属製の鍵自体はあるが、この鍵だけでは開錠できず、通常はこの従来型の鍵を使用せずに、識別記号の送信のみで開錠するように構成しても良い。このような構成とする場合、鍵穴に実際に鍵を差し込んだ状態、あるいは開錠した状態でのみ識別記号の登録変更が出来るようにすると、さらにセキュリティ性が向上する。

【0035】なお、利用者が携帯端末 1 を用いて、ドア 2 の電子錠 3 を開錠する際の手順も、識別記号の登録時と同様、入力キー 12 の中のメニューキー及びカーソルキーを操作し、表示画面 13 に「自宅玄関の鍵をあげる」というような表示をさせる。そして、この画面で、例えば「実行」を選択することにより、上述した識別記号が携帯端末 1 から受信装置 4 へ送信され、電子錠 3 が開錠することとなる。なお、開錠するだけでなく開錠する場合も、このような手順で携帯端末 1 を鍵の代わりに使用するようにしても良い。

【0036】暗証番号の入力を必要とする鍵では、その暗証番号を忘れてしまうと開錠することができなくなってしまうが、上述した本実施の形態のように、携帯端末 1 からの識別記号の送信を利用して開錠を行えるようにすると、このような問題が無くなる。しかも、ある程度高いセキュリティ性が、保証されることとなる。

【0037】次に、第 2 の実施の形態の認証システムについて説明する。この第 2 の実施の形態の認証システムは、図 3 に示すように、携帯端末 1 を用いてコンピュータ 5 のログインを行うものとなっている。すなわち、携帯端末 1 から送信される識別記号を、携帯端末 1 を立てるスタンド型の受信装置 4a が識別して、この携帯端末 1 の所有者を認証した後に、コンピュータ 5 のログインを行う認証システムとなっている。

【0038】携帯端末 1 は、上述した第 1 の実施の形態と同様、通常時は携帯電話としての機能を有したものである。そして、メモリーには、コンピュータ 5 のログインを行うための識別記号を保存することが可能となっている。なお、この第 2 の実施の形態における携帯端末 1 は、底部（図 3 における下部）に識別記号を送信可能な送信部 14a が設けられている。そして、この携帯端末 1 は、コンピュータ 5 に接続されたスタンド型の受信装置 4a に送信部 14a を差し込むことにより、受信装置 4a 上に立てることが可能となっている。そして、このように立てることにより、携帯端末 1 から受信装置 4a に識別記号が送信される。なお、この第 2 の実施の形態

における受信装置 4 a は、送信部 1 4 a を差し込み可能な凹部を有する端子装置となっている。

【0039】受信装置 4 a は、識別記号を受信可能な受信部（図示省略）を備えていると共に、コンピュータ 5 に接続されている。この受信装置 4 a は、立てられた携帯端末 1 から所定の識別記号が所定の送信方法で送信されてくると、これを識別し認証するようになっている。すなわち、携帯端末 1 の所有者をコンピュータ 5 にログインする正当な権利者として認識する。そして、認証したという結果を、コンピュータ 5 に送る。コンピュータ 5 は、携帯端末 1 から送信された信号を正当な識別記号であると受信装置 4 a が認証したことにより、携帯端末 1 の所有者によるログインを開始させるようになっている。

【0040】なお、コンピュータ 5 のログインを行うための識別記号を、携帯端末 1 のメモリに登録し保存させる手順は、上述した第 1 の実施の形態と同様としても良い。しかし、識別記号の設定に関しては、受信装置 4 a の業者から教えてもらうという方法でも良いが、コンピュータ 5 上で設定するようにしても良い。加えて、識別記号を業者から携帯端末 1 に E メールで送ってもらうようにしても良いし、受信装置 4 a の固有の ID 及びそれに対応する識別記号等を管理する管理装置を業者が備え、この管理装置に携帯端末を直接（無線または有線で）接続してメモリに識別記号を保存させるようにしても良い。さらには、出荷時は「0000」のような統一の記号とし、利用前に利用者がログイン用の識別記号の設定を行うようにしても良い。

【0041】なお、上述の第 2 の実施の形態は、携帯端末 1 からの識別記号の送信によってコンピュータ 5 をネットワークにログインさせることとしたが、当該コンピュータ 5 を動作させるオペレーションシステムや各種アプリケーションの起動を当該認証方法を利用して行うようにしても良い。さらには、メールの閲覧時やファイルの閲覧時における個人認証用として、携帯端末 1 からの識別記号の送信を利用するようにしても良い。

【0042】次に、第 3 の実施の形態の認証システムについて説明する。この第 3 の実施の形態の認証システムは、図 4 および図 5 に示すように、各社員が所有する携帯端末 1 a, 1 b, 1 c ……を用いて、各々の職場にて出来勤記録を認識させるものとなっている。すなわち、携帯端末 1 a, 1 b, 1 c ……から送信される識別記号を、各職場の入り口に設けられた受信装置 4 b, 4 c, 4 d ……が識別して、携帯端末 1 a, 1 b, 1 c ……の所有者を認証した後に、その携帯端末の所有者の出退勤記録をとる認証システムとなっている。

【0043】すなわち、図 4 に示すように、各受信装置 4 b, 4 c, 4 d ……は、各携帯端末 1 a, 1 b, 1 c ……を有する各社員の出退勤を認識する出退勤認識装置 6 に接続されている。そして、各受信装置 4 b, 4

c, 4 d ……は、送信されてきた識別記号から、どの携帯端末からの信号かを特定する。各受信装置 4 b, 4 c, 4 d ……は、その識別記号と出勤か退社かの信号と受信時刻等の情報を出退勤認識装置 6 に送る。これにより、出退勤認識装置 6 は、各社員の出退勤時刻等の情報を得て、社員の出退勤を認識する。

【0044】すなわち、図 5 に示すように、出退勤認識装置 6 は、各社員の氏名や所属部署や役職等の社内情報と、各社員に割り振られた識別記号等の携帯端末情報を備えたデータベース 6 1 と、各受信装置 4 b, 4 c, 4 d ……からの情報を受け取る情報受取部 6 2 と、受け取った情報とデータベース 6 1 内の情報とを比較参照する比較手段 6 3 を有している。そして、受信装置 4 b, 4 c, 4 d ……によって特定した識別記号、出退勤の別及び受信時刻等の情報を情報受取部 6 2 で受け取ると、この情報とデータベース 6 1 内の情報とを比較手段 6 3 で比較する。そして、ここで受信した識別記号が存在すると、上述の受信時刻を出勤もしくは退勤時間として出退勤認識装置 6 内に備えられた出退勤簿 6 4 に記録する。

【0045】なお、識別記号のみで一致不一致を識別するのではなく、送信されてきた携帯端末 ID を併せて比較するようにするのが好ましい。この携帯端末 ID を認証の手段として使用する場合は、識別記号を割り振らず、この携帯端末 ID を識別記号として用いることもできる。

【0046】なお、各社員が来社時に携帯する各携帯端末 1 a, 1 b, 1 c ……は、上述した各実施の形態と同様、通常時は携帯電話としての機能を有したものである。そして、メモリには、それぞれの所有者を各職場にて出退勤を認識させるための識別記号を保存することが可能となっている。なお、この第 3 の実施の形態における各携帯端末 1 a, 1 b, 1 c ……は、上述した第 1 の実施の形態と同様、赤外線方式の送信部 1 4 を有している。上述したようにメモリに保存された識別記号は、各社員がそれぞれの職場に到着した際あるいは退社する際に、利用者の操作により送信部 1 4 から赤外線各職場に備えられた各受信装置 4 b, 4 c, 4 d ……に向けて送信される。

【0047】なお、上述した第 3 の実施の形態では出退勤記録だけでなく、各職場への出入り口のドアの開錠を各携帯端末 1 a, 1 b, 1 c ……を利用して行うようにしても良い。この各職場の出入り口となるドアをオートロック式とした場合、開錠後ドアを閉めるとロックされるため、開錠手段を持たない者、すなわち社員ではない部外者の職場への不法侵入を防止することができる。またさらに、各社員が、仕事用に割り当てられたコンピュータのログインも各携帯端末 1 a, 1 b, 1 c ……を利用して行うようにしても良い。このようにすると、仮に部外者の職場への不法侵入を許してしまったとして

も、コンピュータ内の重要なデータの盗み出しや閲覧を防止することができる。なお、上述したように構成する場合、それぞれの行動を可能とする識別記号は、全て共通でも良いし、それぞれ異なっているも良い。

【0048】なお、各職場の受信装置 4 b、4 c、4 d・・・に出退勤を認識させるための識別記号を、各携帯端末 1 a、1 b、1 c・・・のメモリーに登録し保存させる手順は、上述した第 1 および第 2 の実施の形態と同様としても良い。識別記号の設定に関しては、出退勤認識装置 6 を管理する会社側から各社員に与えられた識別記号を、自己の携帯端末 1 a、1 b、1 c・・・に各々が登録するという方法を採用すると、会社側は入力の手間が省ける。しかし、外部へ識別記号が流出する恐れも発生する。

【0049】したがって、セキュリティ性を考慮すると、識別記号の内容を各社員には通知せず、会社側だけで管理し、各携帯端末 1 a、1 b、1 c・・・への入力も会社が行うようにするのが好ましい。加えて、社員が会社を辞める際には、その辞める社員に割り当てた識別記号をメモリーから消去するか、あるいはその識別記号を受信装置 4 b、4 c、4 d・・・が当該会社に属する社員の識別記号として認識しないように受信装置 4 b、4 c、4 d・・・を設定するようにするのが好ましい。

【0050】最後に、第 4 の実施の形態の認証システムについて説明する。この第 4 の実施の形態の認証システム（図示せず）は、携帯端末を用いて自治体の住民票登録管理装置から携帯端末の所有者の個人情報、例えば住民票や印鑑登録証等を引き出すものとなっている。すなわち、携帯端末から送信される識別記号を、自治体の住民票登録管理装置に接続された受信装置が識別し、携帯端末の所有者を認証した後に、その携帯端末の所有者の情報を住民票登録管理装置から引き出す認証システムとなっている。

【0051】なお、この第 4 の実施の形態は、上述した各実施の形態を応用したものであり、例えば、住民票登録管理装置は上述した第 3 の実施の形態の出退勤認識装置 6 とほぼ同様の構成を有している。上述したように構成すると、利用者は、住民票等の証明書の発行を自治体に請求する度に、受付窓口で所定の要件を所定用紙へ書き込むという手間が省ける。また、携帯端末を他人に盗まれたり無くしたりしない限りは、自己の情報を他人に引き出されてしまうという危険も無く、セキュリティ性が保証できる。

【0052】以上の通り、本発明の各実施の形態について説明したが、本発明はこれに限らず、種々の変形、応用が可能である。例えば、現在、銀行の A T M では、カードを機械に挿入し暗証番号入力を行った後に、種々の手続を開始できるようになっているが、その暗証番号入力の部分を携帯端末からの識別記号の送信で代用するようにしても良い。このようにすると、利用者は暗証番号

を忘れて手続ができないという危険を避けられる。

【0053】なお、上述した各実施の形態では、携帯端末から識別記号を受信装置に向けて送信するだけで、受信装置に接続されている各装置を動作させるようにしたが、これにパスワード（暗証番号を含む）入力をさらに要求するようにしても良い。すなわち、上述したパスワード入力を不要とした構成でもある程度高いセキュリティ性があるが、さらにその精度を高くしたい、あるいはさらに信頼性を高めたいというニーズがあることも予想できる。このような場合には、上述した構成に加え、パスワードを入力することにより、受信装置に接続された各装置が所定の動作を行うように構成しても良い。

【0054】パスワードの入力をさらに要求する構成とした場合の処理フローについて、図 6 を用いて説明する。なお、説明にあたり、図 1 の電子錠 3 の開錠を例として説明する。

【0055】まず、携帯端末 1 の所有者は、携帯端末 1 から受信装置 4 へ識別記号を送信する（ステップ S 1 1）。すると、受信装置 4 は識別記号を認識し携帯端末 1 の所有者を認証した後、「パスワードの入力をお願いします」等のメッセージを携帯端末 1 に送信する（ステップ S 1 2）。携帯端末 1 は、このメッセージを表示部となる表示画面 1 3 に表示する（ステップ S 1 3）。このメッセージを読んだ携帯端末 1 の所有者は、携帯端末 1 を用いて予め決められた所定のパスワードを入力し、受信装置 4 に送信する（ステップ S 1 4）。これにより、受信装置 4 が送られてきたパスワードを認証し、接続された装置である電子錠 3 に認証した旨を送信する（ステップ S 1 5）。この結果、電子錠 3 は、携帯端末 1 の所有者の所望の動作を開始する（ステップ S 1 6）。

【0056】なお、上述した例によれば、ステップ S 1 2 でメッセージを携帯端末 1 に送り返し、ステップ S 1 3 で携帯端末 1 がそのメッセージを表示部となる表示画面 1 3 に表示することとしたが、上述のようなメッセージを受信装置 4 が音声で出力するようにしても良い。

【0057】また、上述した例によれば、ステップ S 1 4 で、携帯端末 1 を用いてパスワード入力を行うようにしたが、受信装置 4 にパスワードを入力できる入力手段を設けておくことで、受信装置 4 を操作してパスワード入力をするようにしても良い。

【0058】なお、上述した第 1 の実施の形態では、識別記号の送信方法として赤外線方式を用いたが、無線通信でも良い。また、第 1 の実施の形態の識別記号の送信方法を、第 2 の実施の形態で説明した差し込み式としても良い。また、差し込み式とする場合、上述した第 2 の実施の形態の受信装置 4 a のように、特にスタンド式としなくても良い。単に、携帯端末の送信部の差し込みが可能で、かつデータ送信ができればよい。なお、第 1 および第 2 の実施の形態に限らず、上述した第 3 および第

13

4の実施の形態においても、送信方法として、赤外線方式や無線通信、差し込み式、さらに差し込み式に含まれるスタンド型のいずれを選択しても良い。

【0059】また、上述した各実施の形態では、識別記号の送信手段として、送受信部11とは別に送信部14を設けているが、送受信部11によって識別記号の送信を行うようにしても良い。また、送信部14は、赤外線方式に限定されることはなく、例えば電波、超音波などを利用しても良い。さらには、ケーブル等を利用した有線送信方式としても良い。

【0060】また、上述した各実施の形態では、それぞれ携帯端末を用いて各装置の動作を開始させるための認証を行わせるという説明をしたが、上述した各実施の形態における認証を1台の携帯端末で共通して行えるようにするとより利便性が向上する。なお、そのように構成した場合、各装置に対する認証用の識別記号は共通でも良いし、個別の識別記号をメモリー内に混在させるようにしても良い。その場合、「ドアの開錠」、「ログイン」、「出退勤記録」、「住民票」等の項目を携帯端末の画面に表示させ、その中から所望するものを利用者が選択して識別記号の送信を行うようにしても良い。

【0061】また、上述した各実施の形態において、携帯端末1としては携帯電話が好ましいが、電話機能を有さない携帯端末としても良い。

【0062】

【発明の効果】上述した各発明に係る携帯端末及び認証システムならびに認証方法によれば、携帯端末に装置を動作させるための識別記号を登録しておけば、携帯端末を鍵の代わりとして利用したり、コンピュータのログイン時の認証手段としたりすることができる。しかも、指

14

紋認証等が可能な高コストの設備を取り付けたり、パスワード入力等、人の暗記に頼らずに、確実に装置動作開始時の個人認証を行うことができる。したがって、ある程度高度なセキュリティ性と利便性とを兼ね備えることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態における携帯端末及び認証システムならびに認証方法を説明するためのシステム概念図である。

10 【図2】図1に示した携帯端末に識別記号を登録する手順を示した動作フロー図である。

【図3】本発明の第2の実施の形態における携帯端末及び認証システムならびに認証方法を説明するためのシステム概念図である。

【図4】本発明の第3の実施の形態における携帯端末及び認証システムならびに認証方法を説明するためのシステム概念図である。

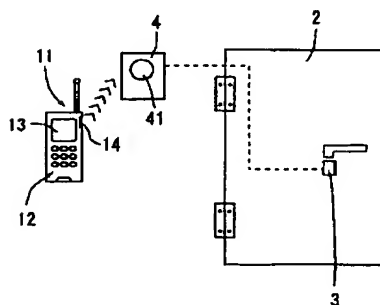
【図5】図4に示した出退勤認識装置の装置構成を示したブロック図である。

20 【図6】本発明の各実施の形態の変形例において、装置の動作を開始させる手順を示した動作フロー図である。

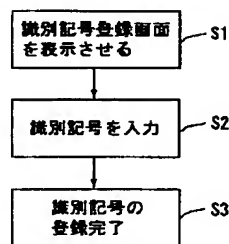
【符号の説明】

- 1 携帯端末
- 2 ドア
- 3 電子錠
- 4, 4a, 4b, 4c 受信装置
- 5 コンピュータ
- 6 出退勤認識装置
- 14 送信部（送信手段）

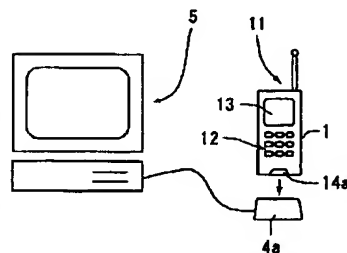
【図1】



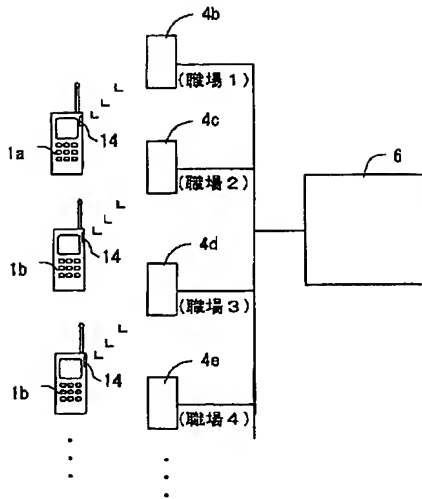
【図2】



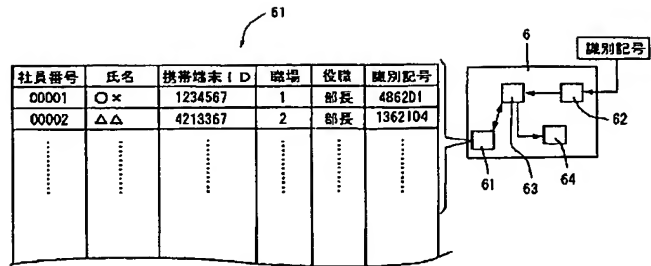
【図3】



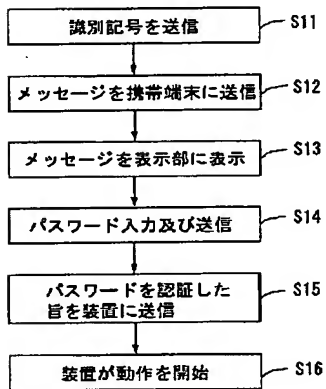
【図 4】



【図 5】



【図 6】



フロントページの続き

F ターム (参考) 2E250 AA02 AA03 AA12 AA14 AA21
 BB08 BB59 BB65 CC26 DD01
 DD06 EE02 FF24 FF36 GG05
 GG08 GG15 HH01 JJ03 KK03
 LL01 TT03
 5B085 AE12 AE13 AE23

THIS PAGE BLANK (USPTO)